Wireless Intrusions and Data Thefts

Gonzalez's Initial Wireless Compromise of BJ's With Scott

Christopher Scott had known Albert Gonzalez since high school when, in 2003, Gonzalez returned home to Miami and began collaborating with Scott on compromising retailers' wireless access points in order to steal and sell track 2 data stored by them.[1]

BJ's Wholesale Club was the first intrusion Scott committed with Gonzalez in order to get track 2 data. The two discovered an open wireless access point at a BJ's Wholesale Club location while "wardriving" – i.e., driving around a neighborhood with a laptop computer equipped with a wireless antenna looking for open wireless access points. The BJ's Wholesale Club's wireless access point was unencrypted and the two were able to place a packet "sniffer" (a program which captures network traffic) on the store's network. Using this first BJ's Wholesale Club location as a beachhead, Gonzalez and Scott moved over the BJ's computer network from store to store via an open and unprotected FTP server, downloading track 2 data from different BJ's stores. (FTP, or file transfer protocol, is a protocol which allows files to be transferred across the Internet.) Gonzalez left Scott to download data from BJ's day after day. Scott gave the downloaded track 2 data to Gonzalez, who in turn sold it. In all, Scott estimates that he and Gonzalez sold at least 300,000 to 400,000 credit card numbers from BJ's. For his work on BJ's,

---

[1] At the request of Scott's defense counsel, the government has endeavored here to identify those facts to which Scott admitted at the time of the search of his residence on May 7, 2008. As acknowledged by Scott in the plea agreement into which he subsequently entered on July 7, 2008, no promises, representations or agreements were made to him other than those set forth in the plea agreement and the proffer agreement dated June 3, 2008. Accordingly, nothing restricts the use of these facts for the purpose of sentencing. In addition, these facts have since been confirmed in material part by the statements of one or more coconspirators.

Statements made by Scott under the protection accorded by the plea and/or proffer agreements have been so identified.

Gonzalez paid Scott approximately $35,000 in cash.[2]

Subsequent Wireless Data Thefts by Gonzalez, Scott and J. J.

After the BJ's intrusion, J. J. became involved in the hacking and downloading, while Gonzalez concentrated on selling the card data and handling the proceeds. Between 2004 and 2007, Scott, J. J. and Gonzalez compromised numerous vulnerable wireless access points, gaining access to the payment card transaction processing networks of OfficeMax, DSW, Sports Authority, Boston Market, Barnes & Noble, TJX Companies ("TJX"), and Target Corporation ("Target").[3] Of these, three – OfficeMax, TJX and Target – require more detailed explication.

OfficeMax

Scott hacked into OfficeMax through a wireless access point with vulnerable WEP encryption and was joined by J. J. in exploiting the vulnerability. (WEP is a data encryption method used to protect data transmitted wirelessly, now widely recognized as flawed.) The OfficeMax intrusion differed from the groups' prior data thefts because the group was able to capture debit card data and PINs, rather than credit card information. The PINs they downloaded were encrypted in a way they did not understand. They gave the debit card data and PINs to Gonzalez, who used an unidentified co-conspirator to break the PINs' encryption scheme. It took the unidentified co-conspirator a year to a year-and-a-half to break the

[2] Scott admitted to committing the BJ's data theft when his house was searched and computer equipment seized pursuant to a search warrant on May 7, 2008. Details contained in this section were fleshed out subsequently by Scott pursuant to the terms of proffer and plea agreements in this case.

[3] Scott admitted at the time of the searches to his involvement in the intrusions into and data thefts from B.J.'s, Sports Authority, and Marshalls, the subsidiary through which TJX financial process server was attacked. The remainder of the victims were identified by him pursuant to the terms of proffer and plea agreements in this case.

encryption, delaying the sale of the carding information.

After the PINs were decrypted, Gonzalez exploited the debit card data both by selling the data in bulk with co-conspirator, Maksym Yastremskiiy ("Maksik"),[4] and "cashing out" the cards directly, through co-conspirator J. W. and others. Gonzalez sold large portions of the stolen debit card identity information to Yastremskiiy, then an international "dumps vendor" (or marketer of track 2 data) living in the Ukraine. At the same time, he used J. W. and others to "cash out" blank debit cards fraudulently imprinted with the stolen data at ATM's in California, Arizona, Pennsylvania and elsewhere.

TJX

Scott initially hacked into TJX's computer network in the summer of 2005 by compromising wireless connection points at two stores owned by TJX's Marshalls subsidiary in Miami, Florida.[5] Within a week or two, Scott had accessed the main TJX servers that processed payment card transactions. Over the coming months, Scott and J. J. downloaded files storing tens of millions of payment card numbers that TJX had stored electronically there. Scott gave the data to Gonzalez for sale.

In the middle of 2006, Scott installed a VPN (virtual private network) connection between TJX's financial transaction processing servers and a server Gonzalez had obtained in California. This let Gonzalez and Scott access TJX over the internet (and eliminating the need to

[4] Maksym Yastremskiiy is under arrest in Turkey and is awaiting extradition in a related case brought by the U.S. Attorney's Office in San Diego.

[5] Scott admitted to hacking Marshalls during the execution of the search warrant at his residence on May 7. He provided the additional details of the TJX intrusion found in this paragraph pursuant to proffer and plea agreements with him.

be in uncomfortably close physical proximity to the Marhalls stores' wireless access points each time they accessed the TJX servers). Contemporaneously, beginning on May 15, 2006, and continuing for some days thereafter, Scott uploaded "sniffer programs" provided him by Gonzalez to a critical TJX payment card transaction processing server. Sniffer programs monitor traffic across a computer network. Gonzalez and Scott sought, and ultimately succeeded, in capturing current, unencrypted credit card data as it traveled across TJX's network while store transactions were being processed. Gonzalez's intimate associate, Stephen Watt, adapted and provided the program – in varying iterations titled "blabla.exe" and "lssas.exe" – for the task.[6]

Target

Toey had moved to Miami in the fall of 2007 at the invitation of Gonzalez, and lived rent free there in Gonzalez's condominium. Gonzalez brought Scott over to the apartment with a specialized high power wireless antenna. (The antenna was still in the condominium when it was searched pursuant to a warrant on May 7, 2008.) Once Scott arrived, Scott connected the antenna to his laptop and began scanning for wireless signals. He was able to locate Target's wireless signal and log on to one of their internal servers using credentials that he had obtained previously. The download on this occasion was overshadowed in size by those of the earlier retailers, and was the last of the conspirators' wireless access points attacks.

[6] While mutually corroborative statements and forensic evidence link Gonzalez, Scott and Watt to the TJX intrusion and data theft, the government is not aware of any evidence linking Toey to the intrusion or data theft, itself. He did, however, sell credit card information stolen from TJX, as summarized above.

The Transition to Internet-Based Security Compromises

While living in Gonzalez's Miami apartment, Toey provided Gonzalez assistance in performing web-based attacks on companies in order to gain access to their computers and information from which the conspirators could benefit, including dumps.

Toey was successful on a number of occasions in gaining access to computer networks over the internet. Typically, Toey sought to gain access to networks through vulnerabilities in the programming of companies' databases, using a technique known as an SQL injection attack. He would then pass the information along to Gonzalez, who would continue hacking the networks himself looking for sensitive financial information, or would pass the information along to another group of hackers for this purpose. By way of example, Toey found a vulnerability in the computer network operated by specialty clothing retailer Forever 21 and gained access to it. He passed the means of access along to Gonzalez, who worked on it with another hacker to obtain payment card information.

Toey also set up computer servers for Gonzalez and his co-conspirators in Latvia and the Ukraine. Gonzalez had root, or unrestricted, access to files on both servers. The Latvian server stored over 16 million distinct credit/debit card numbers. It also contained a folder, to which both Gonzalez and Watt had access, which contained numerous files, including "blabla.exe" and "blabla.c," which possess distinctive features that demonstrate them to be a variants of the same code of the blabla.exe sniffer that had been uploaded to the TJX server in May, 2006, and the Dave and Buster's restaurant chain in 2007. The Ukrainian server contained more than 25

million distinct credit and debit card numbers.[7]

Money and Money Movement

Gonzalez made well over a million dollars from his computer intrusions, data thefts and frauds. Scott made between three hundred and five hundred thousand dollars during the course of the conspiracy;[8] Toey made less – in the area of eighty thousand dollars.

Gonzalez used sophisticated techniques to launder the proceeds of the conspiracy's unlawful activities. For example, Toey generally received payment for dumps that he sold in web currency, internet payment systems designed to conceal the participants in a transaction. On several occasions, Gonzalez instructed Toey to transfer proceeds of the sales of dumps to one of two numbered e-gold web currency accounts which Gonzalez controlled under the user name "segvec." On other occasions, Gonzalez instructed Toey to transfer the proceeds of the sale of dumps to web currency converters Western Express and Roboxchange, who would then wire money to bank accounts controlled by Gonzalez under an alias in Latvia. Gonzalez sent Toey payments via Western Union, which reflected the sender as being a foreign individual Toey did not know. Gonzalez similarly sent Toey cash using a fictitious return address.

Co-conspirator J. W. who “cashed out” hundreds of thousands of dollars from payment cards stolen by Gonzalez and Scott, sent several packages to a mail drop leased by them in the name of an unwitting individual. Scott picked up the packages and split the bundles of cash they contained with Gonzalez. Scott also received an ATM card in a spurious name at this maildrop,

---

[7] The payment card data stored on the servers slightly overlap; there remain, however, more than 40,000,000 distinct payment card numbers stored on the two.

[8] Scott admitted to receiving these payments at the time of the search of his residence.

sent to him from a foreign bank at the direction of Gonzalez. Gonzalez transferred funds to the account backing the ATM card, and Scott used it to repatriate tens of thousands of dollars in payments for his hacking.[9]

[9] The pick-up of packages and the use of the ATM card were described by Scott following his execution of the proffer and plea agreements.